CLAIMS

1.   A method of protecting a digital image, the method comprising:

extracting feature values from the digital image based on a selected authentication bit-rate;

5   embedding data corresponding to the feature values as a watermark into the digital image; and

creating an image signature based on the data corresponding to the feature values.

10   2.   The method as claimed in claim 1, further comprising the step of selecting a desired authentication robustness level, and error correcting coding the extracted feature values prior to embedding the data corresponding to the feature values into the digital image.

15   3.   The method as claimed in claims 1 or 2, wherein the feature values from each of a plurality of codeblocks of the original digital image are thresholded and coded to create the data corresponding to the feature values.

4.   The method as claimed in claim 3, wherein the coding of the
20   thresholded feature values comprises ECC coding to generate parity check bits (PCBs) as the data corresponding to the feature values.

5.   The method as claimed in claim 4, further comprising applying ECC coding again to the PCBs to generate the data corresponding to the feature
25   values.

6.   The method as claimed in any one of claims 1 to 5, wherein the creating of the image signature comprises applying a cryptographic hashing function to a bit sequence representing the data corresponding to the feature
30   values.

7.   The method as claimed in any one of claims 1 to 6, wherein the creating of the image signature comprises utilising a private key.

8.   The method as claimed in any one of claims 1 to 7, wherein the method further comprises distributing the digital image, including the embedded data, as the authentic digital image.

9.   The method as claimed in any one of claims 1 to 8, further comprising coding the digital image, including the embedded data, utilising JPEG2000 compression.

10.   The method as claimed in claim 9, wherein the' extracting of the feature values, the embedding of the data corresponding to the feature values, and
the creating of the image signature are performed as part of the JPEG 2000 coding.

11.   A method of authenticating a digital image, the method comprising:
        extracting data embedded as a watermark in the digital image;
        extracting feature values from the digital image based on a selected authentication bit-rate; and
        processing the extracted data and extracted feature values to derive data corresponding to original feature values; and
        comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.

12.   The method as claimed in claim 11, wherein deriving the data corresponding to the feature values comprises error correcting coding the extracted data and extracted feature values.

13.   The method as claimed in claims 11 or 12, wherein the extracted data and extracted feature values from each of a plurality of codeblocks of the digital image are decoded to derive the data corresponding to the original feature values.

14.   The method as claimed in claim 13, wherein the extracted data comprises PCBs, and the decoding of the extracted data and extracted feature values comprises ECC decoding.

15.   The method as claimed in claim 14, further comprising applying ECC decoding twice to the extracted data.

16.   The method as claimed in any one of claims 10 to 15, further comprising applying a cryptographic technique to the image signature to derive a bit sequence representing the reference data.

17   The method as claimed in any one of claims 10 to 16, further comprising applying a public key to process the image signature for deriving the reference data.

18.   The method as claimed in any one of claims 10 to 17, wherein the method further comprises receiving the digital image as a coded digital image.

19.   The method as claimed in claim 18, wherein the digital image is coded utilising JPEG2000.

20.   The method as claimed in claim 19, wherein the extracting of the data embedded as a watermark, the extracting of feature values from the digital image, the processing of the extracted data and extracted feature values, and the comparing of the derived data corresponding to the original feature values with the reference data are performed as part of the JPEG 2000 de-coding.

21.   A system for protecting a digital image, the system comprising:
a feature value extractor device for extracting feature values from the digital image based on a selected authentication bit-rate;
a watermarking device for embedding data corresponding to the feature values as a watermark into the digital image; and
a processor device for creating an image signature based on the data corresponding to the feature values.

22.   A computer readable data storage medium having stored thereon computer program code means for instructing a computer to execute a method of protecting a digital image, the method comprising:

extracting feature values from the digital image based on a selected
5   authentication bit-rate;

embedding data corresponding to the feature values as a watermark into the digital image; and

creating an image signature based on the data corresponding to the feature values.

10

23.   A system for authenticating a digital image, the system comprising:

an extraction device for extracting data embedded as a watermark in the digital image;

a feature value extractor device for extracting feature values from the
15   digital image based on a selected authentication bit-rate;

a processor device for processing the extracted data and extracted feature values to derive data corresponding to original feature values and for comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.

20

24.   A computer readable data storage medium having stored thereon computer program code means for instructing a computer to execute a method of authenticating a digital image, the method comprising:

extracting data embedded as a watermark in the digital image;
25   extracting feature values from the digital image based on a selected authentication bit-rate;

processing the extracted data and the extracted feature values to derive data corresponding to original feature values; and

comparing the derived data corresponding to the original feature values
30   with reference data derived from an image signature associated with the digital image.